INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

OIPE JC158 AUG 31 2001 PATENT & TRADEMARK OFFICE

ATTY DOCKET NO.	SERIAL NO.
028420-0013CON	09/930,836
P. Kocher et al.	
FILING: August 15, 2001	GROUP: 2132

RECEIVED SEP 05 2001 Technology Center 2100

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
JD		4,908,038 A	3/1990	Matsumura et al.	902	5	
JD		5,297,207 A	3/1994	Degele	380	46	
JD		5,401,950 A	3/1995	Yoshida	235	487	
JD		5,727,063 A	3/1998	Aiello et al.	380	46	
JD		5,778,074 A	7/1998	Garcken et al.	380	37	
JD		5,812,669 A	9/1998	Jenkins et al.	380	25	
JD		5,835,599 A	11/1998	Buer	380	29	
JD		5,838,795 A	11/1998	Mittenthal	380	28	
JD		6,041,412 A	3/2000	Timson et al.	713	200	
JD		6,049,613 A	4/2000	Jakobsson	380	47	
JD		6,064,724 A	5/2000	Kelly	379	92.04	

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

JD			Schneier, Bruce, "Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C," 10/18/95, pages 390-392.
JD			Kocher, P., "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems," in: Koblitz, N., Advances in Cryptology-CRYPTO '96 (Berlin, Springer, 1996), pp. 104-113.

EXAMINER	DATE CONSIDERED
Justin Darrow	06/28/2004

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

OIPE 2100

AUG 31 2001

PATENT & TRADEMARK OFFICE

ATTY DOCKET NO.	SERIAL NO.
028420-0013CON	09/930,836
P. Kocher et al.	
FILING: August 15, 2001	GROUP: 2132

RECEIVED
SEP 05 2001
Technology Center 2100

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
JP		6,064,740	5/2000	Curiger et al.	380	265	
JP		6,069,954	5/2000	Moreau	380	28	

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

JP			"Security Requirements for Cryptographic Modules," Federal Information Processing Standards Publication (FIPS PUB) 140-1, U.S. Department of Commerce, National Institute of Standards and Technology, January 1994.
JP			RSA Data Security, RSAREF Cryptographic Toolkit Source Code, File R-RANDOM C, available from ftp://ftp.rsa.com.

EXAMINER	DATE CONSIDERED
Justin Darrow	06/28/2004

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

Docket Number (Optional)	Application Number
028420-0013CON	09/930,836
Applicant(s)	
P. Kocher et al.	
Filing Date	**Group Art Unit**
August 15, 2001	2132

OIPE SC156
AUG 31 2001
PATENT & TRADEMARK OFFICE

RECEIVED
SEP 05 2001
Technology Center 2100

*EXAMINER INITIAL		OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*
		Krawczyk, H. et al., "HMAC: Keyed-Hashing for Message Authentication," Network Working Group Request for Comments RFC 2104, February 1997.
		Ryan, J., "Blinds for Thermodynamic Cipher Attacks," unpublished material on the World Wide Web at http://www.cybertrace.com/thrmatek.html March 1996.
		"Data Encryption Standard," Federal Information Processing Standards Publication (FIPS PUB) 46-2, U.S. Department of Commerce, National Institute of Standards and Technology, December 30, 1993.
		Biham, E. et al., "Differential Fault Analysis of Secret Key Cryptosystems," in: Kaliski, B., Advances in Cryptology-CRYPTO '97 (Berlin, Springer, 1997), 17th Annual International Cryptology Conference, August 17-21, 1997, pp. 513-525.
		Based on "Karn/Hoey/Outerbridge" implementation (KHODES): "File DESC.C from RSAREF - Data Encryption Standard routines for RSAREF."

EXAMINER	DATE CONSIDERED
Justin Darrow	06/20/2004

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP Section 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.